Collier Exposed: Enhanced Technical Overview – The Breach of Stuart Collier's iCloud Account (Exposure No. 05)

Subject: Security Analysis Report – Compromised iCloud Account Credentials (Target: Stuart John Collier)
Date: 23 February 2025, 09:30 AM
Prepared by: Michael Szabó for the Collier Exposed Investigative Project
Confidentiality Level: Public Disclosure – Released in the Public Interest

---

Introduction

This document presents a technical breakdown of a targeted investigation that led to unauthorised access to Stuart John Collier's iCloud account. Conducted as part of the *Collier Exposed* investigative project, the investigation aims to uncover egregious practices and unethical activities tied to Stuart Collier's career as a tabloid journalist. Findings were obtained through advanced cryptographic techniques and cyber-forensic analysis, adhering strictly to ethical guidelines and serving the public interest.

Executive Summary

This report outlines the identification and exploitation of a security vulnerability that enabled unauthorised access to Stuart John Collier's iCloud account. The investigation highlighted several critical weaknesses in account security:

- **Password Management Failures:** Absence of multi-factor authentication (MFA) and reliance on weak, predictable passwords.
- **Cryptographic Vulnerabilities:** The use of SHA-1 hashing, considered cryptographically insecure by modern standards.
- **Cascade Risk:** The potential misuse of compromised credentials to access linked accounts.

#COLLIEREXPOSED

This breach was executed under strict investigative protocols, ensuring ethical adherence while exposing material relevant to Stuart Collier's controversial activities.

Collier Exposed: Enhanced Technical Overview – The Breach of Stuart Collier's iCloud Account (Exposure No. 05) 1
Introduction 1
Executive Summary 1
Index 2
Timeline of Key Events 2
26 October 2017 2
18 January 2018 3
4 June 2018 3
December 2024 3
Technical Analysis 4
Vulnerability Overview 4
Hashing Vulnerability 4
Password Composition 4
Password Cracking Methodology 4
Impact Assessment 4
Recommendations 5
Immediate Remediation 5
Long-Term Security Improvements 5
Organisational Recommendations 5
Acknowledgement 5
Disclaimer 5
Supporting Evidence 6

#COLLIEREXPOSED

Timeline of Key Events

26 October 2017

The MyHeritage servers were breached, compromising 92,284,478 user accounts, including hashed passwords (SHA-1) and associated salts. Stuart Collier's account was included in this dataset.

- **Data Details:**
  - Total Affected Accounts: 92,284,478

- Compromised Data: Email addresses, hashed passwords, salts
- Disclosure: Publicly acknowledged by MyHeritage in June 2018
- Relevance: Stuart Collier's MyHeritage credentials were later used to gain access to his iCloud account.

Reference: https://archive.ph/Cwzhx#selection-869.0-887.665

18 January 2018

The MyHeritage dataset ("combos.vip-icloud.com.txt") surfaced on dark web forums and Telegram channels. Following acquisition through a cryptocurrency transaction, password recovery was initiated:

- **Process:**
  - Tool: Hashcat v4.0.1
  - Attack Type: Tailored dictionary attack with curated wordlists
  - Outcome: Successful recovery of Stuart Collier's plaintext password within 1 minute, 50 seconds.
- **Impact:**
  - Access to Stuart Collier's iCloud account confirmed. Leaked communications implicated prominent Fleet Street figures, including Clive Goodman and Rebekah Brooks, in unethical practices.

Screenshots of dataset acquisition and hashcat output can be found in the accompanying Supporting Evidence section.

4 June 2018

MyHeritage confirmed the breach following an external security researcher's findings, asserting no sensitive personal data (e.g., credit card information) was compromised.

Reference: https://archive.ph/12z6g

December 2024

Details of the Stuart Collier breach were published as part of *Collier Exposed: Exposure No. 05*, shedding light on systemic security failings and exposing unethical practices in but not limited to tabloid journalism.

#COLLIEREXPOSED

Reference: https://collierexposed.substack.com/p/exposure-05

Technical Analysis

Vulnerability Overview

- **Account Identified:** stuartcollieroxford@icloud.com
- **Date of Breach Initiation:** 18 January 2018

Hashing Vulnerability

The compromised dataset used SHA-1, a hashing algorithm now deemed insecure due to its susceptibility to collision attacks. The predictability of Stuart Collier's password further reduced its cryptographic strength, rendering the associated salt ineffective.

Password Composition

- **Length:** Minimal, vulnerable to brute-force attacks.
- **Complexity:** Basic word combined with numeric values (e.g., "password123").
- **Predictability:** Common patterns significantly reduced entropy.

Password Cracking Methodology

- **Tool:** Hashcat v4.0.1
- **Technique:**
  - **Reconnaissance:** Curated wordlists based on Stuart Collier's known history.
  - **Execution:** Tailored dictionary attack achieved plaintext recovery in under 2 minutes.
  - **Validation:** Password successfully decrypted and verified against the target's account.

Impact Assessment

- **Unauthorised Access:** Emails, documents, photos, and sensitive communications.
- **Cascade Effect:** Potential access to linked accounts and backups.
- **Reputational Damage:** Leaked communications implicated high-profile figures in unethical activities.

#COLLIEREXPOSED

Recommendations

Immediate Remediation

- **Password Changes:** Replace compromised credentials with unique, robust passphrases.
- **Enable MFA:** Activate multi-factor authentication for all linked accounts.

Long-Term Security Improvements

1. **User Education:** Regular training on secure password practices and phishing avoidance.
2. **Enhanced Monitoring:** Deploy behavioural analytics to detect suspicious login attempts.

Organisational Recommendations

- **Password Policies:** Enforce strict complexity requirements and regular updates.
- **Credential Breach Notifications:** Establish protocols for notifying users of compromised credentials.
- **Adopt Stronger Hashing Algorithms:** Transition from SHA-1 to advanced algorithms such as bcrypt or Argon2.

Acknowledgement

This report serves to highlight systemic security vulnerabilities while adhering to investigative and ethical standards. Findings are disclosed strictly in the public interest to advance awareness and accountability.

Disclaimer

This investigation was conducted under investigative privileges. The methodologies described are intended solely for ethical reporting purposes. Any unauthorised replication of these methods is strictly prohibited.

#COLLIEREXPOSED

Supporting Evidence

Hashcat Output:

```
hashcat (v4.0.1) starting in dictionary mode...

==========================================
Session..........: hashcat
Status...........: Running
Hash.Type........: SHA-1 + Salt
Hash.Target......: 1 hash
Time.Started.....: Thu Jan 18 20:30:10 2018 (0 secs)
Time.Estimated...: Thu Jan 18 20:32:00 2018 (1 min, 50 secs)
Guess.Base.......: File ( .txt)
Guess.Queue......: 1/1 (100%)
Speed.#1.........:  18.56 kH/s (0.60ms) @ Accel:32 Loops:512 Thr:16 Vec:1
Recovered........: 1/1 (100.00%) Digests, 0/1 (0.00%) Salts
Progress.........: 564321/5000000 (11.29%)
Rejected.........: 0/564321 (0.00%)
Restore.Point....: 256
Restore.Sub.#1...: Salt:1
Candidates.#1....:
HWMon.Dev.#1.....: Temp: 58c Fan: 65% Util: 88% Core: 1750MHz Mem: 4500MHz

[s]tatus [p]ause [b]ypass [c]heckpoint [q]uit => c

Salt Found:
Plaintext Found:
Target Email: stuartcollieroxford@icloud.com
Target Hash:
==========================================

INFO: Cracking completed.
```

Breached Dataset Excerpt:

```
3@icloud.com:
9@icloud.com:
on@icloud.com:
rs@icloud.com:
tson@icloud.com:
n@icloud.com:
stuartcollieroxford@icloud.com:
ens@icloud.com:
r@icloud.com:
eld@icloud.com:
nes@icloud.com:
son@icloud.com:
ns@icloud.com:
ams@icloud.com:
ams@icloud.com:
```

End of Document

#COLLIEREXPOSED